

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)20702 CRESCENT POINT PLACE
ASHBURN, VIRGINIA

Case No. 1:20-SW-980

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

20702 Crescent Point Place, Ashburn, Virginia, as further described in Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1343

Wire Fraud

Offense Description

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

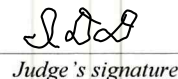
Reviewed by:
 James P. Gillis
 Assistant United States Attorney


 Applicant's signature

Javier A. Gonzalez, Special Agent, FBI
 Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ (specify reliable electronic means).

Date: 08/05/2020


 Judge's signature

City and state: Alexandria, Virginia

Hon. Ivan D. Davis, United States Magistrate Judge
 Printed name and title

ATTACHMENT A

Premises To Be Searched

The premises to be searched, 20702 Crescent Point Place, Ashburn, Virginia, is located at the intersection of Crescent Point Place and Rock Harbor Circle. It is a two-story structure with a brick veneer front facade, vinyl siding on the sides, a composite shingle roof, and a side-by-side two-car garage with a white garage door. A photograph of the premises and a map showing its location are shown below:



ATTACHMENT B

Particular Things To Be Seized

- A. All documents or information constituting or referring or relating to any financial instrument, including but not limited to any stocks, stock options, commodities, commodity futures, and any other instrument traded on public or private exchanges.
- B. All documents or information referring or relating any financial account, including but not limited to any checking, savings, loan, line of credit, credit card, brokerage, or trading account.
- C. All documents or information constituting or referring or relating to tax returns and schedules; IRS forms, such as Form W-2 and Form 1099; and documents used in the preparation of taxes.
- D. All documents or information referring or relating to any of the following:
 - 1. Arca Enterprises Inc.,
 - 2. Bim4sites LLC,
 - 3. Brevon Developers Inc.,
 - 4. Ignite Beverage Corp.,
 - 5. LAD Marketing Group LLC,
 - 6. Monument Communications LLC.
 - 7. PDK Building & Design LLC,
 - 8. Square Capital LLC,
 - 9. Square Inc.,
 - 10. TMC Partners LP,
 - 11. United Canna Corp, LLC
 - 12. United Canna LLC,
 - 13. Wall Street Fusion Group,
 - 14. Austin Jacobs,
 - 15. Clyde Kessler,

16. Daniel Coyle,
17. David Baker,
18. Domenick Alario,
19. Donald Hartman,
20. Earl Burger,
21. Jason Goldsberry,
22. Jeffrey Boogaard,
23. Jorge Diaz,
24. Nico Mastrangelo,
25. Paul Apostolopoulos,
26. Sam Grant,
27. Samuel Dealey,
28. Sandra Vass,
29. Stephanie Dosik, or
30. Thomas Coyle.

- E. All documents or information referring or relating to any person(s) who interacted or communicated with Brett Amendola about matters relating to any investment, business, transfer of any funds or things of value, checking, savings, loan, line of credit, credit card, brokerage, or trading account, or about Brett A. Amendola's employment history or experience, including documents or information that help reveal the identity or whereabouts of the person(s).
- F. All documents or information referring or relating to the Paycheck Protection Program or the Small Business Administration, including any submitted or required to be submitted to obtain any loan or guarantee, such as income tax records, monthly payroll expenses, number of employees, interest on mortgages, rent, and utilities.
- G. The information, documents and things that may be seized pursuant to this warrant may be seized in whatever form, visual or aural, and by any means by which they may have been created, stored, or found, including electronic form, such as any computer, mobile telephone, laptop, tablet, or other electronic device or medium of any kind, including any components

or attachments, that may contain any of the information, documents, and things that may be seized pursuant to this warrant.

H. For any computer, mobile telephone, laptop, tablet, or other electronic device or medium of any kind, including any components or attachments, the seizure of which is otherwise authorized by this warrant (collectively “electronic device”):

1. evidence of who used, owned, or controlled the electronic device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the electronic device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the electronic device was accessed or used to determine the chronological context of electronic device access, use, and events relating to crime under investigation and to the electronic device user;
5. evidence indicating the electronic device user's state of mind as it relates to the crimes under investigation;
6. evidence of the attachment to the electronic device of other storage devices or similar containers for electronic evidence;
7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic device;
8. evidence of the times the electronic device was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the electronic device;
10. documentation and manuals that maybe necessary to access the electronic device or to conduct a forensic examination of the electronic device;
11. records of or information about Internet Protocol addresses used by the electronic device;

12. records of or information about the electronic device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
13. Routers, modems, and network equipment used to connect any electronic device to the Internet.

During the execution of the search of the person, place, or thing described in the preceding attachment, law enforcement officials executing the search are authorized to use the facial features and fingerprints of Brett A. Amendola, and those of any person found in or upon the place or thing to be searched, to “unlock” any device that may be seized pursuant to this warrant and that may be subject to biometric security measures. The procedure for using such biometric features may include holding the device close to the face of the person, pressing the fingers and thumbs of the person to the device, and shall otherwise be comparable to those used in routine booking procedures. This warrant **does not authorize the use of force** to effect the use of the person’s biometric features, and should the person refuse to comply, the government must apply to the Court for an order to require compliance.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.